UNITED STATES DISTRICT COURT

for the

District of Utah

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

INFORMATION ASSOCIATED WITH THE GOOGLE ACCOUNT tyimckinlay@gmail.com STORED AT PREMISES CONTROLLED BY GOOGLE LLC

Case No. 4:25-mj-00071 PK

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A, incorporated herein by reference.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 2252A	Transportation/Receipt/Distribution/Possession of Child Pornography

The application is based on these facts:

See attached Affidavit, incorporated herein by reference.

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

IVAN J MURRAY
Digitally signed by IVAN J MURRAY
Date: 2025.07.02 14:48:44 -06'00'

Applicant's signature

HSI SA Ivan Murray

Printed name and title

Sworn to before me and signed in my presence.

Date: July 2, 2025

Judge's signature

City and state: St. George, Utah

United States Magistrate Judge Paul Kohler

Printed name and title

FELICE JOHN VITI, Acting United States Attorney (#7007)
CHRISTOPHER BURTON, Assistant United States Attorney (NV #12940)
Attorneys for the United States of America
Office of the United States Attorney
20 North Main Street, Suite 208
St. George, Utah 84770
Telephone: (435) 634-4270
Christopher.Burton4@usdoj.gov

IN THE UNITED STATES DISTRICT COURT

DISTRICT OF UTAH

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE GOOGLE ACCOUNT tyimckinlay@gmail.com THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE LLC.	AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEARCH WARRANT Case No. 4:25-mj-00071 PK

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Ivan Murray, Special Agent with Homeland Security Investigations, being duly sworn, state:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises owned, maintained, controlled, or operated by Google LLC ("Google"), an electronic communications service and/or remote computing service provider headquartered at 1600

Amphitheater Parkway, Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with Homeland Security Investigations and have been since November of 2011. I am currently assigned to assist the Federal Bureau of Investigation's Child Exploitation Task Force (CETF) as well as the Utah Attorney General's Internet Crimes Against Children Task Force (ICAC). Prior to my current position with HSI, I was employed as a Criminal Investigator/Special Agent with Internal Revenue Service - Criminal Investigative Division for approximately seven years. I've received training in child-pornography investigations, and I've had the chance to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have received additional training from CETF and ICAC relating to online, undercover chatting investigations, as well as peer-2-peer or P2P investigations. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. Specifically, I have participated in numerous investigations relating to the sexual exploitation of children over the Internet since 2013.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18 U.S.C. § 2252A(a)(5) (Possession of child pornography); 18 U.S.C. § 2252A(a)(1) (Transportation of child pornography); and 18 U.S.C. § 2252A(a)(2), (Distribution/Receipt of child pornography) have been committed by TYI MCKINLAY. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and fruits of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

6. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively, and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types—to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer—can store thousands of images or videos at very high resolution. It

is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

g. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as "apps." Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to interact directly with other like-

minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored.

h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO HAVE A SEXUAL INTEREST IN CHILDREN OR WHO PRODUCE, RECEIVE, AND/OR POSSESS CHILD PORNOGRAPHY

7. Based on my previous investigative experience related to child-exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who have a sexual interest in children and/or produce, receive, or possess images of child pornography:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children

engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain child pornographic material in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain those materials and child erotica for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography images, which are valued highly. Often, these offenders will maintain a collection on multiple devices. However, some individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.[1]

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain contact information (e.g., online messaging accounts, email addresses, etc.) of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

8. Based on all of the information contained herein, I believe that MCKINLAY likely displays characteristics common to individuals who have a sexual interest in children and/or receive or possess images of child pornography.

---

[1] *See United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); *see also United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370-71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010)).

DETAILS OF THE INVESTIGATION

9. On or about April 1, 2025, the National Center for Missing and Exploited Children received an investigative lead from Google (CyberTip 208457740). The CyberTip provided information that a Google user had uploaded suspected child sexual abuse material ("CSAM") onto Google servers. The CyberTip provided the following suspect information:

> Name: Tk
> Mobile Phone: +13852752221 (Verified 01-15-2025 19:04:50 UTC)
> Mobile Phone: +19286128385 (Verified 04-28-2022 20:12:34 UTC)
> Date of Birth: 08-04-1981
> Email Address: tyimckinlay@gmail.com (Verified)
> Email Address: glowbiz10@gmail.com

10. I know, based on my training and experience, that the phrase "verified" as it relates to the suspect email address indicates the particular email address has been verified to be the suspect email account associated with the illegal activity and that additional email addresses listed (such as glowbiz10@gmail.com) are associated with the suspect account and are likely recovery accounts. The CyberTip indicated that at least 1,668 files of confirmed CSAM had been located on Google's servers. The CyberTip also provided geolocation information for the phone numbers associated with the suspect account. The listed customer for phone number 928-612-8385 was Steven Fitch of Surprise, Arizona. The listed customer for phone number 385-275-2221 was MCKINLAY of Kanab, Utah. MCKINLAY's phone number was the most recent verified phone number associated with the accounts. NCMEC also provided geolocation information for various internet protocol ("IP") addresses associated with the suspect

account, which included IP addresses in Kanab as well as various other locations in Utah, Washington, California, and Oregon.

11. On April 5, 2025, NCMEC received a second CyberTip from Google regarding the same suspect (CyberTip 208638354). The second CyberTip indicated that at least 103 files of CSAM had been located on Google's servers and listed the same suspect information:

> Name: Tk
> Mobile Phone: +13852752221 (Verified 01-15-2025 19:04:50 UTC)
> Mobile Phone: +19286128385 (Verified 04-28-2022 20:12:34 UTC)
> Date of Birth: 08-04-1981
> Email Address: tyimckinlay@gmail.com (Verified)
> Email Address: glowbiz10@gmail.com

12. The second CyberTip listed the same customers for the associated phone numbers and listed IP addresses associated with the suspect in Kanab, Utah, as well as other locations in Utah, Washington, Oregon, and California.

13. Investigators received both CyberTips in May 2025. Investigators reviewed some of the files from both CyberTips that had already been reviewed by Google employees. Those files depicted CSAM, and two examples of such files (one from each CyberTip) are described below:

> **Name:** fcd64e8b29df9a9c11a477b38b45efa3.jpg
> **Description:** This image depicts a completely nude Caucasian female, between five and seven years of age, seated and spreading her legs so that her vagina is partially visible. She is viewed looking to one side and holding long strands of her hair in each of her hands.
>
> **Name:** 7ee76696de947620f89abaf88507ff97-WGGI
> **Description:** This file is a video that is 6 minutes and 24 seconds in length. Throughout the video a Caucasian female,

> between 8 and 10 years of age, routinely exposes her vagina and anus to the camera's lens. Throughout the video the female will routinely use her fingers to masturbate.

14. Investigators attempted to identify MCKINLAY, given his name was included in the verified suspect email account and he was the listed customer for the most recent verified phone number associated with the suspect account. Investigators learned that MCKINLAY had a DOB of 8/4/1981, matching the suspect information provided in both CyberTips, and was a registered sex offender. MCKINLAY was convicted in 2004 of sexual exploitation of a minor and sexual abuse of a child, both felonies, in the Fifth Judicial District Court for the State of Utah. MCKINLAY's registered address was 160 E. 200 N. in Kanab, the same listed with his verified phone number in both CyberTips.

15. On May 28, 2025, officers stopped MCKINLAY as he was driving and executed a State search warrant for his phone.[2] MCKINLAY's cell phone was found in MCKINLAY's possession and was seized at that time pursuant to the State search warrant. Officers also *Mirdandized* and interviewed MCKINLAY. During that interview, MCKINLAY admitted to using his cell phone to download "kiddie porn." MCKINLAY admitted that the downloaded files would still be present on that cell phone. MCKINLAY also confirmed that the email address tyimckinlay@gmail.com (the "Subject Account") belonged to him.

[2] This affidavit is not relying on the State search warrant or the results of any subsequent search in establishing probable cause to search the Subject Device.

BACKGROUND CONCERNING GOOGLE[3]

16. Google is a United States company that offers to the public through its Google Accounts a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether or not they have a Google Account, a free web browser called Google Chrome, a free search engine called Google Search, a free video streaming site called YouTube, a free mapping service called Google Maps, and a free traffic tracking service called Waze. Many of these free services offer additional functionality if the user signs into their Google Account.

17. In addition, Google offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Google also sells devices, including laptops, mobile phones, tablets, smart speakers, security cameras, and wireless routers. Users of Android and Google devices are prompted to connect their device to a Google Account when they first turn on the device, and a Google Account is required for certain functionalities on these devices.

18. Signing up for a Google Account automatically generates an email address at the domain gmail.com. That email address will be the log-in username for access to the Google Account.

---

[3] The information in this section is based on information published by Google on its public websites, including, but not limited to, the following webpages: the "Google legal policy and products" page available to registered law enforcement at lers.google.com; product pages on support.google.com; or product pages on about.google.com.

19. Google advertises its services as "One Account. All of Google working for you." Once logged into a Google Account, a user can connect to Google's full suite of services offered to the general public, described in further detail below. In addition, Google keeps certain records indicating ownership and usage of the Google Account across services, described further after the description of services below.

20. Google integrates its various services to make it easier for Google Accounts to access the full Google suite of services. For example, users accessing their Google Account through their browser can toggle between Google Services via a toolbar displayed on the top of most Google service pages, including Gmail and Drive. Google Hangout, Meet, and Chat conversations pop up within the same browser window as Gmail. Attachments in Gmail are displayed with a button that allows the user to save the attachment directly to Google Drive. If someone shares a document with a Google Account user in Google Docs, the contact information for that individual will be saved in the user's Google Contacts. Google Voice voicemail transcripts and missed call notifications can be sent to a user's Gmail account. And if a user logs into their Google Account on the Chrome browser, their subsequent Chrome browser and Google Search activity is associated with that Google Account, depending on user settings.

21. When individuals register with Google for a Google Account, Google asks users to provide certain personal identifying information, including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.

22. Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was created, the length of service, log-in times and durations, the types of services utilized by the Google Account, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website or using a mobile application), details about the devices used to access the account, and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the account and accept Google's terms of service, as well as the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the Google Account.

23. Google maintains the communications, files, and associated records for each service used by a Google Account on servers under its control. Even after a user deletes a communication or file from their Google Account, it may continue to be available on Google's servers for a certain period of time.

24. In my training and experience, evidence of who was using a Google account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

25. Based on my training and experience, messages, emails, voicemails, photos, videos, documents, and internet searches are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to a Google Account may provide direct evidence of the offenses under investigation.

26. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Google can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

27. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (*e.g.,*

information indicating a plan to commit a crime), or consciousness of guilt (*e.g.,* deleting account information in an effort to conceal evidence from law enforcement).

28. Other information connected to the use of a Google account may lead to the discovery of additional evidence. For example, the apps downloaded from the Google Play store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

29. Therefore, Google's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Google services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

CONCLUSION

30. Based on the forgoing, I request that the Court issue the proposed search warrant.

31. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it,

reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

RESPECTFULLY SUBMITTED this 2nd day of July, 2024.

IVAN J MURRAY

Digitally signed by IVAN J MURRAY
Date: 2025.07.02 14:47:35 -06'00'

Ivan Murray, Special Agent
Homeland Security Investigations

Subscribed and sworn to before me this 2nd day of July, 2024.

JUDGE PAUL KOHLER
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with tyimckinlay@gmail.com ("the Account") that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google LLC ("Google")

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Google, Google is required to disclose to the government for each account or identifier listed in Attachment A the following information from January 1, 2025, through present, unless otherwise indicated:

a. All business records and subscriber information, in any form kept, pertaining to the Account, including:

1. Names (including subscriber names, user names, and screen names);
2. Addresses (including mailing addresses, residential addresses, business addresses, and email addresses, including alternate and recovery email addresses);
3. Telephone numbers, including SMS recovery and alternate sign-in numbers;
4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions, including log-in IP addresses;
5. Telephone or instrument numbers or other subscriber numbers or identities, including any temporarily assigned network address, SMS recovery numbers, Google Voice numbers, and alternate sign-in numbers
6. Length of service (including start date and creation IP) and types of service utilized;

7. Means and source of payment (including any credit card or bank account number); and

8. Change history.

b. All device information associated with the Account, including but not limited to, manufacture names, model numbers, serial number, media access control (MAC) addresses, international mobile equipment identifier (IMEI) numbers, FCC ID numbers, Android IDs, and telephone numbers;

c. Records of user activity for each connection made to or from the Account(s), including, for all Google services, the date, time, length, and method of connection, data transfer volume, user names, source and destination IP address, name of accessed Google service, and all activity logs

d. Emails sent or received by the Account, including those that have been deleted or exist only in the "drafts" folder of the Account.

e. Any media associated with the Account, to include any photographs or videos.

Google is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and/or instrumentalities of violations of Title 18 U.S.C. § 2252A(a)(5) (Possession of child pornography); 18 U.S.C. § 2252A(a)(1) (Transportation of child pornography); and 18 U.S.C. § 2252A(a)(2) (Distribution/Receipt of child pornography), those violations involving TYI MCKINLAY and occurring after January 1, 2025, including, for each Account or identifier listed on Attachment A, information pertaining to the following matters:

a. Child pornography, as defined by 18 U.S.C. 2256(8);

b. Evidence indicating how and when the Account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

c. Evidence indicating the Account owner's state of mind as it relates to the crime under investigation;

d. The identity of the person(s) who created or used the Account, including records that help reveal the whereabouts of such person(s).

e. The identity of the person(s) who communicated with the Account about matters relating to the possession, transport, receipt, or distribution of child pornography, including records that help reveal their whereabouts.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google LLC ("Google"), and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google. The attached records consist of _____. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google, and they were made by Google as a regular practice; and

b. such records were generated by Google's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Google, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date	Signature